PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-237484
(43)Date of publication of application : 23.08.1994

(51)Int.Cl. H04Q 7/04

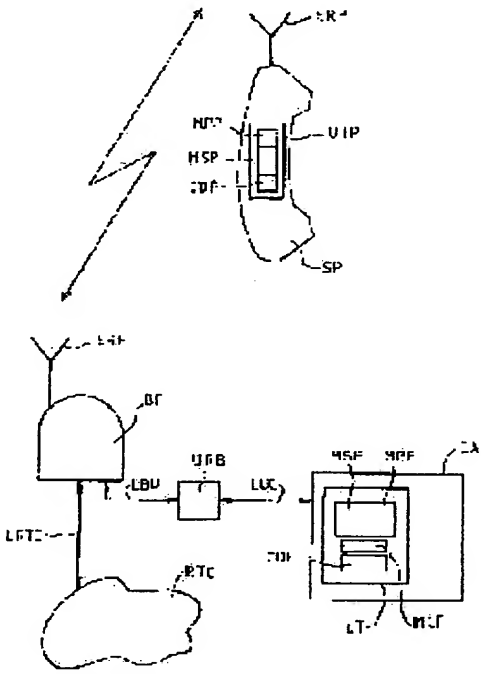
(21)Application number : 03-126287
(22)Date of filing : 29.05.1991

(71)Applicant : FR TELECOM
(72)Inventor : LANGRAND FRANCK
MAZZIOTTO GERALD
BAUDOUX SOPHIE

(30)Priority
Priority number : 90 9006662 Priority date : 29.05.1990 Priority country : FR

(54) TELEPHONE SYSTEM FOR REMOTELY LOADING TELEPHONE SUBSCRIPTION DATA OF ISOLATED STATION

(57)Abstract:
PURPOSE: To obtain a device and method having high safety with respect to illegal telephone connection, using existing basic facilities and remotely load telephone subscription data.
CONSTITUTION: A controlling means UTF searches all of telephone subscription data regarding an isolated station SP and data, that shows the orders of remote loading based on a call request LID from the station SP. A coding means CDF encodes a secret data PIN. A processing means sends open data and secret data to an independent station. The independent station decodes the secret data and stores it in a memory.



LEGAL STATUS

[Date of request for examination]	02.10.1995
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	2685661
[Date of registration]	15.08.1997
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's	

.decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平6－237484

(43)公開日　平成６年(1994)８月23日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｑ　7/04		Ｃ　7304－5Ｋ		

審査請求　未請求　請求項の数19　ＯＬ　（全 15 頁）

(21)出願番号　特願平3－126287

(22)出願日　平成３年(1991)５月29日

(31)優先権主張番号　９０　０６６６２

(32)優先日　1990年５月29日

(33)優先権主張国　フランス（ＦＲ）

(71)出願人　591044452
フランス　テレコム
ＦＲＡＮＣＥ　ＴＥＬＥＣＯＭ
フランス国，92131　イシレムーリノー
ル　デュ　ジェネラル　レックラーク38－
40番地

(72)発明者　フランク・ラングラン
フランス国、エフ－75013　パリ、リュ・
ビュオ、19

(72)発明者　ジェラール・マジョット
フランス国、エフ－75014　パリ、リュ・
デュ・ムラン・ベール、56

(74)代理人　弁理士　筒井　大和　（外１名）

最終頁に続く

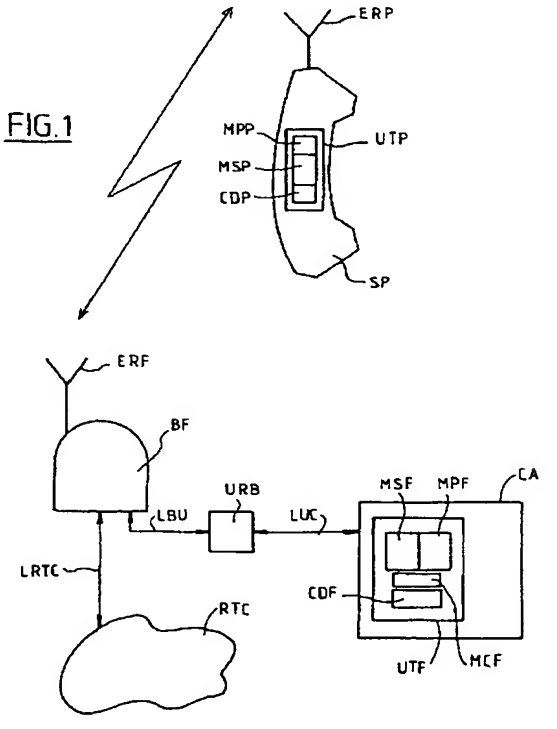
(54)【発明の名称】　独立局の電話加入データの遠隔ローディングのための電話装置

(57)【要約】

【目的】　不正電話接続に対する安全性の高い、また、現在の基礎施設を用いることのできる電話加入データの遠隔ローディングのための装置と方法の提供。

【構成】　独立局（ＳＰ）からの呼び出し要求（ＬＩＤ）に応じて、制御手段（ＵＴＦ）が独立局（ＳＰ）に関するすべての電話加入データおよび遠隔ローディングの順序を示すデータをサーチする。コード手段（ＣＤＦ）は秘密データ（ＰＩＮ）をコード化する。処理手段は独立局に公開データおよび秘密データを送信する。独立局は秘密データをデコードし、メモリーに格納する。

FIG.1



1

【特許請求の範囲】

【請求項１】　－　交換電話ネットワーク（ＲＴＣ）に接続された少なくとも１つの固定ターミナル；

－　少なくとも１つの独立局（ＳＰ）で、該独立局からの呼び出し要求の後に前記固定ターミナル（ＢＦ）と遠隔相互通信可能な少なくとも１つの独立局；該独立局は次の処理手段（ＵＴＰ）を有する、すなわち：

・　前記独立局（ＳＰ）に関する電話加入データを格納することを意図したメモリー（ＭＰＰ、ＭＳＰ）、および、

・　データをコード化／デコードする手段；

－　前記固定ターミナルに接続され、前記電話加入データを電話接続を妨げる目的で制御することができる処理手段を設けた、認証手段（ＣＡ）、を有する電話装置であって、

前記認証手段の前記処理手段は：

－　前記独立局に関する電話加入データおよび該電話加入データが該独立局に遠隔的にロードされなければならないことを示すことのできるデータを保持することのできるメモリー（ＭＰＦ、ＭＳＦ）、

－　前記独立局のため少なくとも１つの特別キーを選択できる手段を備えた、変数キーデータのコード／デコード手段（ＣＤＦ）；

－　要求により、前記独立局を特定することにより電話加入データをサーチすることのできる制御手段（ＭＣＦ）、を有し、

前記認証手段（ＣＡ）の側においては、

・　前記独立局（ＳＰ）から到来する、呼び出し要求のための公開数値ワード（ＬＩＤ）と該独立局を特定するための公開数値ワード（ＰＩＤ）に応じて、また、電話加入データの遠隔ローディングに関する所定の条件を確証するロード要求信号の存在のもとで、制御手段（ＵＴＦ）が該独立局（ＳＰ）に関しすべての電話加入データおよび遠隔ローディングの順序を示すデータをサーチし、

・　前記コード／デコード手段（ＣＤＦ）が前記特別キー（ＥＰＩＤ）すなわち秘密特別キー（ＰＩＮ）を用いてコード化し、

・　前記遠隔ローディングの順序を示すデータの値に応じて、処理手段（ＵＴＦ）がコード化されない公開電話加入データおよび前記コード化された秘密電話加入データを前記独立局（ＳＰ）に送信し、

他方、前記独立局（ＳＰ）の側では、

・　コード／デコード手段（ＣＤＰ）は、受け取った前記コード化された秘密電話加入データを特別キー（ＥＰＩＤ）を用いて解読し、そして

・　処理手段（ＵＴＰ）は送信された秘密でない前記電話加入データおよび解読された秘密電話加入データを前記独立局のメモリーに格納する、ことを特徴とする電話装置。

2

【請求項２】　前記ロード要求信号が前記独立局からの信号であることを特徴とする請求項１の装置。

【請求項３】　前記独立局からの前記ロード要求信号が、前記呼び出し要求のための公開数値ワード（ＬＩＤ）を該独立局（ＳＰ）のキーボードに入力することからなることを特徴とする請求項２記載の装置。

【請求項４】　前記ロード要求信号が前記認証手段からの信号であることを特徴とする請求項１の装置。

【請求項５】　秘密でない前記公開電話加入データおよびコード化された前記秘密データの送信に引き続いて、前記認証手段の前記処理手段が認証要求のための公開数値ワード（ＡＵＴＨ＿ＲＥＱ）をランダムキーワード（ＲＡＮＤ）と共に前記独立局に引き渡し；該認証要求のための公開数値ワード（ＡＵＴＨ＿ＲＥＱ）に応じて、前記独立局の前記コード／デコード手段（ＣＤＰ）が、受け取った前記ランダムキーワードを遠隔ロードされた前記秘密電話加入データ（ＰＩＮ）を用いてコード化し、該独立局のための付加的な特別キーを生成し、

前記独立局が前記コード化されたランダムキーワード（ＣＰＩＮ）を認証応答のための数値ワード（ＡＵＴＨ＿ＲＥＳ）と共に前記認証手段に送信し、

該認証応答のための数値ワード（ＡＵＴＨ＿ＲＥＳ）に応じて、前記認証手段（ＣＡ）の前記コード／デコード手段（ＣＤＦ）が前記コード化されたランダムキーワード（ＣＰＩＮ）を解読し、このようにデコードされた該ランダムキーワードを生成された前記ランダムキーワードと比較し、比較結果に応じて、電話加入データがロードされることを示すデータを前記独立局に格納し、電話接続を生成する、ことを特徴とする請求項１ないし４のいずれか１項の装置。

【請求項６】　前記秘密電話加入データが前記独立局の個人特定番号（ＰＩＮ）であることを特徴とする請求項１ないし５のいずれか１項の装置。

【請求項７】　前記公開電話加入データが、前記呼び出し要求のための公開数値ワード（ＬＩＤ）、オペレータ特定のための数値ワード（ＯＰＳＩＣ）、前記独立局のサービスクラスに関する数値ワード（ＴＣＯＳ）、そして加入のための数値データ（ＴＲＤ）からなることを特徴とする請求項１ないし６のいずれか１項の装置。

【請求項８】　前記コード／デコード手段が前記独立局の前記個人特定番号（ＰＩＮ）を変数データ（ＥＰＩＮ１、ＥＰＩＮ２）、および暗号関数Ｆによる前記特別キー（ＥＰＩＤ）を用いた該変数データ（ＥＰＩＮ１、ＥＰＩＮ２）の変換（Ｓ１、Ｓ２）に応じてコード化／デコードすることを特徴とする請求項６の装置。

【請求項９】　前記コード／デコード手段が前記独立局の前記個人特定番号（ＰＩＮ）を、変数データ（ＥＰＩＮ１、ＥＰＩＮ２）および、該変数データの暗号関数Ｆによる、特別キー（ＥＰＩＤ）および付加的な変数データ（ＥＰＩ３）を用いた変換（Ｓ１、Ｓ２）に応じてコ

3

ード化／デコードすることを特徴とする請求項６の装置。

【請求項１０】　前記独立局が、補助的認証手段（ＣＡＡ）がデータの交換を目的として前記認証手段（ＣＡ）と接続された、補助的交換電話ネットワークと遠隔相互通信ができ、該補助的認証手段の処理手段（ＵＴＦＡ）が：

－　前記独立局に関する仮電話加入データを保持することのできるメモリー（ＭＰＦＡ、ＭＳＦＡ）；

－　前記独立局のための該仮電話加入データを生成することができる制御手段（ＭＣＦＡ）；を有し、そして、前記認証手段（ＣＡ）の側では、

・　前記補助的電話ネットワーク（ＣＡＡ）との接続要求のための公開数値ワード（ＲＯＡＭＩＮＧ）に応じ、該接続要求のための公開数値ワード（ＲＯＡＭＩＮＧ）が認証手段による前記独立局の認証に関する所定の条件を確証する時、前記処理手段が変数データ（ＥＰＩＮ１、ＥＰＩＮ２）を生成し、秘密電話加入データにより形成された特別キー（ＰＩＮ）を用いて該変数データの変換（Ｓ１、Ｓ２）を計算し、

・　前記処理手段（ＵＴＦ）が前記変数データ（ＥＰＩＮ１、ＥＰＩＮ２）および計算された該変数データの変換（Ｓ１、Ｓ２）を前記補助的認証手段（ＣＡＡ）に送信し；

前記補助的認証手段の側では、

・　前記制御手段（ＭＣＦＡ）が仮公開電話加入データを生成し；

・　前記制御手段が仮秘密電話加入データ（ＲＰＩＮ）を生成し、受け取った前記変数データ（ＥＰＩＮ１、ＥＰＩＮ２）および該変数データの前記変換（Ｓ１、Ｓ２）を用いて該仮秘密電話加入データをコード化し、

・　処理手段（ＵＴＦＡ）がコード化された前記仮秘密電話加入データを生成された前記公開仮電話加入データと共に前記独立局へ送信し、

前記独立局（ＳＰ）の側では、

・　前記コード／デコード手段（ＣＤＰ）が、受け取ったコード化された前記仮秘密電話加入データを、前記秘密電話加入データにより生成された前記特別キー（ＰＩＮ）を用いて解読し、そして、

・　前記処理手段（ＵＴＦ）が、受け取った秘密でない前記公開仮電話加入データおよびコード化された前記秘密データを前記メモリー（ＭＰＰ、ＭＳＰ）に格納する、ことを特徴とする請求項１ないし９のいずれか１項の装置。

【請求項１１】　前記仮秘密電話加入データが前記独立局の前記個人特定番号（ＲＰＩＮ）からなることを特徴とする請求項１０の装置。

【請求項１２】　前記公開電話加入データが、前記呼び出し要求のための公開数値ワード（ＬＩＤ）、前記オペレータの特定のための数値ワード（ＯＰＳＩＣ）、前記

4

独立局のサービスクラスに関する数値ワード（ＴＣＯＳ）、そして前記加入の数値データ（ＴＲＤ）からなることを特徴とする請求項１０および１１のいずれか１項の装置。

【請求項１３】　前記コード／デコード手段が前記独立局の前記仮個人特定番号（ＲＰＩＮ）を前記変数データ（ＥＰＩＮ１、ＥＰＩＮ２）、および前記特別キー（ＰＩＮ）を用いた暗号関数Ｆによる該変数データの前記変換（Ｓ１、Ｓ２）に応じてコード化／デコードすることを特徴とする請求項１１の装置。

【請求項１４】　前記コード／デコード手段が、前記独立局の前記仮個人特定番号（ＲＰＩＮ）を、前記変数データ（ＥＰＩＮ１、ＥＰＩＮ２）、および前記特別キー（ＰＩＮ）ならびに前記補助的認証手段の制御手段により生成された付加的な変数データ（ＥＰＩＮ３）を用いた暗号関数Ｆによる該変数データの前記変換（Ｓ１、Ｓ２）に応じてコード化／デコードすることを特徴とする請求項１１の装置。

【請求項１５】　前記認証手段（ＣＡ）あるいは前記補助的認証手段（ＣＡＡ）が、すべての前記独立局および前記交換ネットワーク（ＲＴＣ）あるいは前記補助的交換ネットワーク（ＳＴＣＡ）のすべての前記固定ターミナルのための一般認証センターと通じることを特徴とする請求項１ないし１４のいずれか１項の装置。

【請求項１６】　前記認証手段（ＣＡ）あるいは前記補助的認証手段（ＣＡＡ）が固定ターミナルに収容され、前記独立局のすべて、および前記交換ネットワーク（ＲＴＣ）あるいは前記補助的交換ネットワーク（ＲＴＣＡ）の前記固定ターミナルのすべてのための一般認証センターと接続されていることを特徴とする請求項１ないし１４のいずれか１項の装置。

【請求項１７】　請求項１ないし９、１５、１６のいずれか１項の電話装置に利用されることを目的とする、電話加入データの遠隔ローディングの方法であって、認証手段（ＣＡ）の処理手段には：

－　独立局に関する電話加入データおよび該電話加入データが該独立局に遠隔ローディングされなければならないことを示すことのできるデータを通信により保持することができるメモリー（ＭＰＦ、ＭＳＦ）；

－　前記独立局のための少なくとも１つの特定キーを選択できる手段を備えた、変数キーデータのコード／デコード手段（ＣＤＦ）；

－　要求により、前記独立局を特定することにより前記電話加入データをサーチすることができる制御手段（ＭＣＦ）；が設けられ、

次のステージ、すなわち：

ａ）　前記認証手段（ＣＡ）の側において、

・ａ１）前記独立局（ＳＰ）からの呼び出し要求のための公開数値ワード（ＬＩＤ）と該独立局の特定のための公開数値ワード（ＰＩＤ）に応じて、また、電話加入デ

5

ータ遠隔ローディングに関する所定の条件を確証する要求信号の存在のもとで、該独立局（ＳＰ）に関するすべての前記電話加入データおよび遠隔ローディングの順序を示すデータをサーチし、

・ａ２）特別キー（ＥＰＩＤ）を用いて秘密データ（ＰＩＮ）をコード化し、

・ａ３）遠隔ローディングの順序を示すデータの値に応じて、秘密でない公開加入データおよびコード化された前記秘密データを前記独立局（ＳＰ）に送信し、

ｂ）　前記独立局（ＳＰ）の側において、

・ｂ１）受け取ったコード化された秘密電話加入データを特別キー（ＥＰＩＤ）を用いてデコードし、

・ｂ２）送信された秘密でない前記公開電話加入データおよびデコードされた前記秘密電話加入データを前記独立局（ＳＰ）の前記メモリーに格納する、からなる、ことを特徴とする電話加入データの遠隔ローディング方法。

【請求項１８】　請求項１０ないし１６のいずれか１項の電話装置に利用されることを目的とする、電話加入データの遠隔ローディングの方法であって、前記独立局は、補助的認証手段（ＣＡＡ）がデータ交換ができるため認証手段（ＣＡ）に接続された補助的交換電話ネットワークと遠隔相互通信でき、

該補助的認証手段（ＣＡＡ）の処理手段（ＵＴＦＡ）には：

－　前記独立局に関する仮電話加入データを保持できるメモリー（ＭＰＦＡ、ＰＳＦＡ）；

－　前記独立局のための仮公開電話加入データを生成することができる制御手段（ＭＣＦＡ）；が設けられ、

次のステージ、すなわち：

１）　前記認証手段（ＣＡ）の側においては、

・１１）前記補助的認証手段（ＣＡＡ）から前記補助的電話ネットワークへの接続要求のための公開数値ワード（ＲＯＡＭＩＮＧ）に応じて、該接続要求のための公開数値ワード（ＲＯＡＭＩＮＧ）が前記認証手段による独立局の認証に関する所定の条件を確証する時、変数データ（ＥＰＩＮ１、ＥＰＩＮ２）を生成し、秘密電話加入データにより生成された特別キー（ＰＩＮ）を用いて該変数データの変換（Ｓ１、Ｓ２）を計算し、

・１２）前記変数データ（ＥＰＩＮ１、ＥＰＩＮ２）および計算された該変数データの前記変換を補助的認証センター（ＣＡＡ）に送信し、

２）前記補助的認証手段の側においては、

・２１）前記仮公開電話加入データを生成し、

・２２）仮秘密電話加入データ（ＲＰＩＮ）を生成し、前記変数データ（ＥＰＩＮ１、ＥＰＩＮ２）および該変数データの前記変換（Ｓ１、Ｓ２）を用いて該仮秘密電話加入データをコード化し、

・２３）コード化された前記仮秘密電話加入データを、生成された前記仮公開電話加入データと共に前記独立局に送信し、

6

３）　前記独立局（ＳＰ）の側では、

・３１）受け取ったコード化された前記仮秘密電話加入データを、前記秘密電話加入データにより生成された前記特別キー（ＰＩＮ）を用いて解読し、そして、

・３２）受け取った秘密でない前記仮公開電話加入データおよびデコードされた秘密データを前記メモリー（ＭＰＰ、ＭＳＰ）に格納すること、からなる、ことを特徴とする電話加入データの遠隔ローディング方法。

【請求項１９】　ステージ２２が付加的な次のステージ、すなわち：

＊２２１）付加的な変数データ（ＥＰＩＮ３）を生成し、補足的な該変数データ（ＥＰＩＮ３）をさらに用いて前記電話加入データをコード化する、ステージをさらに含むことを特徴とする請求項１８の方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、独立局の電話加入データの遠隔ローディングに関する。本発明は、ＧＳＭ（特別移動グループ、Group Special Mobile）、ＤＣＴ（ディジタルコードレス電話、Digital Cordless Telephone）と呼ばれるシステムおよび無線インタフェースＣＡＩ（共通無線インタフェース、Common Air Interface）のような、移動あるいは固定独立局を有する電話通信システム、特にフランスのポアンテル（POINTEL 、登録商標）システムにおいて実施することができる。

【０００２】

【従来の技術】一般的に言って、そのような通信システムは、交換電話ネットワークに接続された少なくとも１つの固定ターミナル、および、自分からの呼び出し要求の後にその固定ターミナルと遠隔相互通信が可能な少なくとも１つの独立局を有している。

【０００３】非常にしばしば、独立局の特定はその独立局の電話加入データにより決定される。

【０００４】電話接続の要求が独立局から送信される時はいつでも、電話加入データに応じて電話接続の生成を妨げることのできる、交換ネットワークに接続された認証センターにより、独立局からの電話加入データが統制されている。

【０００５】実際的には、不正電話接続の発生を避けるため、電話加入データの少なくとも１部は秘密あるいは機密要素を有している。

【０００６】ＮＭＴ（北欧移動電話、Nordic Mobile Telephone ）やＲＡＤＩＯ　ＣＯＭ２０００と呼ばれるシステムのような第一世代の移動独立局を有する電話通信システムにおいては、電話設備の取付者あるいはセールスマンにより電話加入データが移動独立局にロードされた。

【０００７】

【発明が解決しようとする課題】このローディング方法

は次のような問題を有する。すなわち、商業的な供給における適応性と融通性の不十分さ、電話設備のセールスマンとサービス提供者の役割の混同、そして、不正接続に対する低レベルの安全防護、である。

【０００８】ＧＳＭのような第二世代の移動独立局を有する電話通信システムにおいては、着脱可能な加入モジュールに電話加入データがプログラムされていることを考えている。この解決は前記のローディング方法により多くの安全性を付与するという点で優れている。それにもかかわらず、着脱可能な加入モジュールに加入データをプログラムすることは特別の設備によってなされるので、電話加入権の分配のために大きな基礎施設が必要である。

【０００９】本発明はこの問題を解決することを本質的な目的としている。

【００１０】

【課題を解決するための手段】このように、本発明の１つの目的は、独立局からの電話加入データの遠隔ローディングの方法を提供することである。

【００１１】本発明は、次のものを有する電話装置に関するものである。すなわち：

－　交換電話ネットワークに接続された少なくとも１つの固定ターミナル；

－　自分からの呼び出し要求の後に固定局と遠隔相互通信の可能な少なくとも１つの独立局であって、次の処理手段を有する独立局；

・　その独立局に関する電話加入データを格納できるメモリー、そして、

・　コード／デコード手段；

－　固定局に接続され、電話接続の開始を妨げるため電話加入データを制御することのできる処理手段を備えた認証手段。

【００１２】本発明の一般的な定義によれば、認証手段の処理手段は次のものを有している；すなわち、

－　独立局に関する電話加入データ、およびその電話加入データが前記独立局に遠隔ローディングされるべきことを示すことのできるデータを格納することができるメモリー；

－　独立局のための少なくとも１つの特別キーの選択を可能にする手段と共に、変数キーデータをコード／デコードするための手段；

－　要求に応じて、独立局を特定することにより電話加入データをサーチすることのできる制御手段；そして認証手段のレベルにおいては、

・　独立局の特定の公開数値ワードと共に独立局から発信される呼び出し要求の公開数値ワードに応じて、そして電話加入データの遠隔ローディングに関する所定の条件を実証するロード要求信号の存在のもとで、制御手段は独立局に関するすべての電話加入データを、遠隔ローディングの順序に関するデータと共にサーチし、

・　コード／デコード手段は特別キーを用いて秘密データをコード化し、

・　処理手段は秘密ではない公開電話加入データをこのようにコード化された秘密データと共に、遠隔ローディングの順序を示すデータの値に応じて、独立局に送信することを許可し、独立局のレベルにおいては、

・　コード／デコード手段は受け取ったコード化された秘密電話加入データを特別キーの助けにより解読し、

・　処理手段は、コード化されずに送信された秘密ではない公開電話加入データとデコードされた秘密データを独立局のメモリーに格納する。

【００１３】このような装置は、電話加入データのプログラムあるいは遠隔ローディングのための特別の設備を必要とせず、現存の通信ネットワークの基礎施設を電話加入権の分配や管理のために使用することができる。

【００１４】さらに、秘密電話加入データをコード化して送信することにより、この電話加入データの遠隔ローディングの安全性を非常に高いものにする。

【００１５】本発明の好ましい実施例によれば、ロード要求信号は独立局から発信される信号である。

【００１６】実際的には、独立局から発信される要求信号は、呼び出し要求のための公開数値ワードを独立局のキーボードに入力することからなっている。

【００１７】本発明の他の実施例によれば、ロード要求信号は認証手段から発信される信号である。

【００１８】本発明の他の側面によれば、秘密ではない公開電話加入データのコード化されない送信ならびにコード化された秘密データの送信の後に、認証に関する処理手段は独立局に対し認証要求のための公開数値ワードと欄ダムキーワードを送信し、認証要求のための数値ワードに応じて、独立局のコード／デコード手段はこのように受け取ったランダムキーワードを、遠隔ロードされた秘密電話加入データを用いてコード化し、この独立局に特定のもう１つのキーを作り出し、独立局はこのコード化されたランダムキーワードを認証手段に、認証応答のための数値ワードと共に、送信し、そして、この認証応答のための数値ワードに応答して、認証手段のコード／デコード手段はこのように受け取ったコード化されたランダムキーワードをデコードし、デコードされたランダムキーワードを生成されたランダムキーワードと比較し、この比較に応じて、電話加入データが独立局にロードされていることを示すデータを格納し、電話接続を実現する。

【００１９】実際的には、秘密電話加入データは独立局の個人特定番号からなっている。

【００２０】実際的には、公開電話加入データは呼び出し要求のための公開数値ワード、オペレータの数値識別ワード、独立局のサービスクラスに関する数値ワードおよび数値加入データを含むものである。

【００２１】本発明の他の側面によれば、コード／デコ

ード手段は、変数データおよび暗号関数Ｆによるその変換に応じ、特別キーと付加的な変数データの助けを得て独立局の個人特定番号をコード化／デコードする。

【００２２】本発明の１変形によれば、独立局は補助的交換電話ネットワークと遠隔相互通信が可能であり、その補助的交換電話ネットワークの補助的認証手段は認証手段と互いの間でデータの交換ができるように接続されており、補助的認証手段の処理手段が、次のものを有していることを特徴とする、すなわち、

－　独立局に関する仮電話加入データを格納することができるメモリー；

－　独立局のための仮電話加入データを生成することができる制御手段；そして、認証手段のレベルでは、

・　補助的認証手段から発信される補助的電話ネットワークとの接続要求のための公開数値ワードに応じて、接続要求のための公開数値ワードが認証手段による独立局の認証に関する所定の条件を実証するとき、処理手段は変数データを生成し、秘密電話加入データから形成された特別キーの助けによりその変換を計算し、

・　処理手段は変数データおよびこのように計算されたその変換を補助的認証手段に送信し；補助的認証手段のレベルでは、

・　制御手段が仮公開電話加入データを生成し、

・　制御手段は仮秘密電話加入データを生成し、それを受け取った変数およびその変換によりコード化し、

・　処理手段はこのようにコード化された仮秘密電話加入データを生成された仮公開電話加入データと共に独立局に送信し、独立局のレベルでは、

．　コード／デコード手段が、受け取ったコード化された秘密電話加入データを、秘密電話加入データにより形成された特別キーの助けにより解読し、処理手段はコード化されないで受け取った秘密でない仮公開電話加入データ、およびデコードされた秘密データをメモリーに格納する。

【００２３】このような装置は、先に認証手段と補助的認証手段の間で秘密電話加入データを送信することなく補助的認証手段のレベルで秘密電話加入データを生成することができ、また、それにより仮電話加入データの遠隔ローディングの安全性が高まるという点で有利である。

【００２４】仮秘密電話加入データを独立局の仮個人特定番号とするのが実際的である。

【００２５】実際的には、仮公開電話加入データは、呼び出し要求のための公開数値ワード、オペレータの数値特定ワード、独立局のサービスクラスに関する数値ワード、そして数値加入データからなるものとすることができる。

【００２６】本発明の他の側面によれば、コード／デコード手段は、独立局の仮個人特定番号を変数データ、ならびに特別キーを用いたその変数データの暗号関数Ｆによる変換に応じてコード化／デコードする。

【００２７】コード／デコード手段が独立局の仮個人特定番号を、変数データ、特別キーを用いた暗号関数Ｆによるその変換、および補助的認証手段の制御手段により生成された付加的な変数データに応じてコード／デコードするのは有利である。

【００２８】本発明の他の特徴によれば、認証手段あるいは補助的認証手段が、すべての独立局ならびに交換ネットワークあるいは補助的交換ネットワークのすべての固定ターミナルのために機能する一般認証センターと通じるものである。

【００２９】本発明の他の特徴によれば、認証手段あるいは補助的認証手段は固定ターミナルに収納され、すべての独立局ならびに交換ネットワークの固定ターミナルのための一般認証センターに接続されている。

【００３０】本発明は、電話装置で用いられることを意図した電話加入データの遠隔ローディング方法を含むものである。

【００３１】本発明の方法によれば認証手段の処理手段には次のもの、すなわち：

－　独立局に関する電話加入データおよびその電話加入データがその独立局に遠隔ロードされなければならないことを示すことができるデータを、通信により、格納できるメモリー；

－　独立局のための少なくとも１つの特別キーの選択を可能にする手段を備えた、変数キーデータをコード／デコードするための手段；

－　要求に応じ、独立局を特定することにより電話加入データをサーチすることができる制御手段、を設けることが提案され、この方法は次のステップ、すなわち：

ａ）認証手段のレベルにおいて、

・ａ１）独立局からの公開特定数値ワードと共に、また、制御信号の存在のもとで、独立局から発信される呼び出し要求のための公開数値ワードに応じて、電話加入データの遠隔ローディングに関する所定の条件を検証し、独立局に関するすべての電話加入データならびに遠隔ローディングの順序を示すデータをサーチし、

・ａ２）秘密の特別キーデータの助けを得てコーディングし、

・ａ３）遠距離ローディングを示すデータの値に対応して、秘密ではない公開の電話加入データをコード化しないまま、そして秘密データはコード化して前記独立局に送信することを許可し、

ｂ）独立局のレベルにおいて、

・ｂ１）受け取った秘密電話加入データを特別キーを用いてデコードし、

・ｂ２）送信された秘密でない公開加入データ、ならびにデコードされた秘密データを独立局のメモリーに格納する、ことからなるものである。

【００３２】本発明の特に興味深い変形として、本発明

の電話加入データの遠隔ローディング方法は、補助的認証手段が認証手段との間でデータの交換を可能にする目的でその認証手段と接続されている補助的交換電話ネットワークと独立局が遠隔相互通信できる電話装置にも適用することができる。

【００３３】この変形方法においては、補助認証手段の処理手段は次のもの、すなわち：

－　独立局に関する仮電話加入データを格納することができるメモリー；

－　独立局のための仮電話加入データを生成することができる制御手段；を備えており、そして、この方法が次のステップ、すなわち：

１）認証手段のレベルにおいて、

・１１）補助的認証手段から発信される補助的電話ネットワークとの接続要求のための公開数値ワードに応じて、接続要求のための公開数値ワードが独立局の認証に関する認証手段による所定の条件を証明した場合、変数データを生成し、秘密電話加入データにより形成される特別キーを用いてその変換を計算し、

・１２）変数データならびに前記のように計算されたその変換を補助認証手段に送信し、

２）補助認証手段のレベルでは、

・２１）仮公開電話加入データを生成し、

・２２）仮秘密電話加入データを生成し、変数データならびにその変換を用いてその仮秘密電話加入データをコード化し、

・２３）このようにコード化された仮電話加入データを、生成された公開仮電話加入データと共に、独立局に送信し、

３）独立局のレベルでは、

・３１）受け取られたコード化された秘密電話加入データを秘密電話加入データを用いてデコードし、そして、

・３２）受けとられたコード化されていない仮公開電話加入データおよびデコードされた秘密データをメモリーに格納する、ことからなるものを考えることができる。

【００３４】ステージ２２がさらに次のステップ、すなわち：

＊２２１）付加的な変数データを生成し、電話加入データをさらにこの補足的な変数データを用いてコード化する、ことからなるものとするのは有利である。

【００３５】本発明の他の特徴および有利な点は以下の詳細な説明とそれに関連する図面からより一層明らかになるであろう。

【００３６】

【実施例】図１はアングロサクソンの規格であるＣＡＩ（共通無線インタフェース、Common Air Interface）のＭＰＴ１３７５規格に基づくポアンテル（POINTEL 、登録商標）タイプの遠距離通信ネットワークに用いられることを意図した電話装置を示す線図である。

【００３７】移動可能なあるいは固定の独立局ＳＰは、

独立局ＳＰからの呼び出し要求を経て、固定ターミナルＢＦと遠隔遠距離通信を行なうことができる。独立局ＳＰは送受信機およびアンテナを有する組立体ＥＲＰを備えている。

【００３８】固定ターミナルＢＦの側には、固定ターミナルと独立局間の遠隔相互通信のための送受信機およびアンテナを有する組立体ＥＲＦが設けられている。

【００３９】ＣＡＩ規格の規定によれば、独立局と固定ターミナル間の無線伝送手段は、電話チャンネル（Ｂ）および数値信号チャンネルＤから構成されている。

【００４０】固定ターミナルは交換電話ネットワークＬＲＴＣに接続されている。ＣＡＩ規格の規定によれば、独立局は：

－　独立局からの公開電話加入データを格納するための公開メモリー領域ＭＰＰと、その独立局からの秘密電話加入データを格納するための秘密メモリー領域ＭＳＰとに分割されたメモリー、および、

－　データのコード／デコード手段ＣＤＰ、を有する処理手段ＵＴＰを備えている。

【００４１】独立局のメモリーをプロテクトされた領域とプロテクトされていない領域に分割することは安全性を高めるために有益であることに注目できる。しかし、この分割は本発明の実施のために必須ではない。

【００４２】最後に、本装置にはターミナル接続ユニットＵＲＢを介して固定ターミナルに接続された認証手段ＣＡが設けられている。特定電話接続ＬＢＵにより、ターミナル接続ユニットＵＲＢと固定ターミナルＢＦとの結合が可能とされており、他方、数値信号線（ＬＵＣ）により認証手段ＣＡとターミナル接続ユニットＵＲＢとの結合が可能とされている。

【００４３】認証手段ＣＡは、独立局からの電話加入データを保持し、固定ターミナルと独立局の間の電話接続の成立を阻止するため電話加入データを制御できるメモリーを備えた処理手段ＵＴＦからなっている。認証手段のメモリーが、独立局からの公開電話加入データを格納できる公開メモリー領域、およびその独立局の秘密電話加入データを格納できる秘密メモリー領域ＭＳＦに分割するのは有利である。

【００４４】勿論、この分割は本発明の実施に必須のものではない。

【００４５】ここで、認証手段ＣＡはすべての独立局および交換ネットワークＲＴＣの固定ターミナルのための一般認証センターに対応することができることに注目すべきである。

【００４６】また、認証手段が少なくとも１つの固定ターミナルに収納され、それがすべての独立局および交換ネットワークＲＴＣの固定ターミナルのための一般認証センターに接続されている、独立局を有する遠隔通信システムが存在し得ることにも注目できる。

【００４７】以下の説明において、認証手段が交換ネッ

13

トワークの認証センターに対応する通信システムだけが考慮される。しかし、本発明のこの本質的な要素手段は固定ターミナルに収容される認証手段にも適用することができる。

【００４８】ポアンテル（POINTEL 、登録商標）からの電話加入データは加入契約の際にポアンテルの契約担当者から加入者に割り当てられる。このデータは独立局がポアンテル・サービスにアクセスするのを認められるのに必要である。

【００４９】ＣＡＩ規格によれば、電話加入データは次のものを含んでいる、すなわち：

－　無線接続を確立するため固定ターミナルに送られる最初のパケットのビットに対応する、呼び出し要求のための公開数値ワードＬＩＤ（リンク特定データ、Link Identification Deta）、このサイズは１６ビットである；

－　独立局の秘密特定番号に関する数値ワードＰＩＮ（個人特定データ、Personal Identification Number）、このサイズは６４ビットである；

－　オペレーションの特定のための数値ワードＯＰＳＩＣ（オペレータ特定コード、Operators Identity Code）、このサイズは９ビットである；

－　独立局のサービスのクラスに関する数値ワードＴＣＯＳ（サービスの通信クラス、Telecom Class of Service）、サイズは３ビット；そして、

－　それだけで独立局の加入を特定する目的のための付加的電話加入データに関する数値データＴＲＤ（通信ポイント登録データ、Telepoint Registration Data ）、サイズは最大８０ビット。

【００５０】ＣＡＩ規格によれば、無線電話接続を実現するために、数値ワードＬＩＤ、ＰＩＮ、ＯＰＳＩＣおよびＴＣＯＳが必須である。ＣＡＩ規格はこれらのワードのサイズも規定している。他方、ワードＴＲＤについてはオペレータの裁量に委ねられている。例えば１０進コードとしてもよい。

【００５１】他方、ワードＯＰＳＩＣは加入が承認されたポアンテル契約者を特定するものである。

【００５２】一般的に言って、電話加入データは、それが割り当てられた後、ポアンテル呼び出しの際、要求されたサービスを提供する前に、独立局を認証するために用いられる。

【００５３】当面、ＣＡＩ規格は、電話設備の取付者あるいはセールスマンによる、独立局の電話加入データのマニュアルローディングを規定している。

【００５４】今では、そのような電話加入データのローディング方法は、電話設備のセールスマンあるいは加入者からのマニュアルな介入が必要であり、不正な加入に対する安全性が低いという点で、不満足なものである。

【００５５】出願人は、ポアンテル型の電話装置の基礎構造を修正すること無しに、上記の問題点を解決することのできる、電話加入データの遠隔ローディング方法を提供するという問題に直面した。

14

【００５６】図２および図３は本発明による電話加入データの遠隔ローディングのプロトコルの必須な要素段階を線図により示したものである。

【００５７】遠隔ローディングのプロトコルは、独立局から発せられる呼び出し要求に関するＥ１ステージにより開始される。

【００５８】Ｅ１ステージは、固定ターミナルＢＦとの無線接続を確立することを目的として独立局において受話器をフックから外すことにより開始される。アクセスはランダムであり、ＣＡＩ規格により割り当てられる４０のチャンネルのうちの１つを介して達成される。無線接続は、呼び出し要求のための公開数値ワードＬＩＤが交換された電話ネットワークにより受理された時に、固定ターミナルＢＦとの無線接続が確立される。

【００５９】ステージＥ２において、独立局は固定局との間で互いに補足し合うメッセージを交換し、これにより独立局を認証できる。

【００６０】より具体的に言えば、独立局は独立局の能力に関するメッセージＴＥＲＭ＿ＣＡＰ（ターミナル能力情報要素、Terminal Capabilities Information Element）と独立局の活動に関するメッセージＦＡ３，ｎ（特徴活動情報要素、FeatureActivation Information Element）を発する。メッセージＴＥＲＭ＿ＣＡＰおよびＦＡ３，ｎにより独立局は固定ターミナルに対し自分自身を表示することができる。

【００６１】メッセージＴＥＲＭ＿ＣＡＰおよびＦＡ３，ｎに応じて、固定ターミナルは、独立局のスクリーンを消去する命令に関するメッセージＤＩＳＰ＝ＦＦ、およびその後（ステージＥ２３およびＥ２４において）認証されるという条件で、（この場合メッセージＦＡ３，ｎにより）要求されたサービスを受理するメッセージＦ１３，ｎを送る。

【００６２】そのほかに、固定ターミナルＢＦは、固定ターミナルにより認証された、独立局の電話能力に関するメッセージＢＡＳ＿ＣＡＰ（基底能力情報要素、Base Capabilities Information Element ）を発する。

【００６３】Ｅ２３ステージの時に、固定ターミナルはランダムなキーワードＲＡＮＤを生成し、このランダムキーワードＲＡＮＤを認証要求に関する公開数値ワードＡＵＴＨ＿ＲＥＱと共に独立局に発信する。

【００６４】認証要求のための数値ワードＡＵＴＨ＿ＲＥＱに応じて、独立局のコード／デコード手段ＣＤＰは受け取ったランダムキーワードＲＡＮＤを独立局用の特別なキーの助けを得てコード化する。例えば、特別のキーはその独立局の秘密電話加入データ、特にその個人特定番号ＰＩＮ、により作成することができる。

【００６５】次に、独立局はこのようにコード化されたランダムキーワードＣＰＩＮを認証の応答のための公開

15

数値ワードＡＵＴＨ＿ＲＥＳと共に固定ターミナルＢＦに送る。独立局は、独立局のメモリーに秘密電話加入データＰＩＮが無い結果、ランダムワードのコード化が無効である場合、認証されないと考えられる。

【００６６】他方、秘密電話加入データＰＩＮが独立局のメモリーにある場合、独立局の認証に関するステージＥ２は肯定的なものとなり、認められた電話接続が生成される結果となる。

【００６７】更に詳しく説明すると、認証の応答のための数値ワードＡＵＴＨ＿ＲＥＳに応答して、認証センターのコード／デコード手段ＣＤＦは受け取ったランダムキーワードコードＣＰＩＮを、特別のキーＰＩＮの助けを得て解読し、このようにデコードしたランダムキーワードを固定ターミナルにより生成されたランダムキーワードと比較し、その比較結果に基づいて電話接続の生成を認める。

【００６８】ステージＥ３は独立局のキーボードからの呼び出し番号の列挙からなっている。

【００６９】ここで、これら３つのステージＥ１ないしＥ３は現行のＣＡＩ規格にすでに存在しているものであることに注目できる。

【００７０】本発明によれば、ステージＥ３に引き続いて、ステージＥ４が考慮されるが、それは次のように展開する。

【００７１】まず第１に、認証センターは固定ターミナルから、第１の呼び出しを行ないたいと希望している、独立局の特定情報を受け取る。この特定情報はワードＰＩＤ、ＴＣＯＳ、ＯＰＳＩＣ、ＴＲＤおよびＬＩＤからなるメッセージを送ることが含まれている。次いで、認証センターはワードＬＩＤ、ＦＡ３，ｎにより、そして電話呼び出しの場合は希望の電話番号により、求められているサービスを決定する（ステージ４１）。

【００７２】呼び出し要求のための数値ワードＬＩＤに応じて認証センターは独立局から発せられている呼び出し要求に答えるべきかどうか決定する。

【００７３】非常に有利なことに、本発明によれば、ＬＩＤが電話加入データの遠隔ローディングの要求を伴った呼び出し要求に関する場合、それを見分けることができる。

【００７４】例えば、電話加入データの遠距離ローディングを希望する場合、電話加入データの遠距離ローディングのための特別なＬＩＤをキーボードに入力することが考えられる（ＬＩＤのマニュアル生成）。

【００７５】ここで、ＣＡＩ規格によればＬＩＤは０から７までででなる４桁の数字であり、１６進では０００００から０３ＥＦまででである、ことに注目できる。

【００７６】本発明によれば、さらに、電話加入データが独立局へ遠隔的にロードされるべきであることを示すデータは、認証センターの処理手段のメモリーに格納されるべきである、ことを考えることができる。

16

【００７７】まず第１に、独立局から、独立局からの特定ＰＩＤと共に、電話加入データの遠隔ローディングに関する所定の条件を証明するロード要求信号の存在のもとに発せられる呼び出し要求ＬＩＤ（ここではＬＩＤのマニュアル生成）に応答して、制御手段は、独立局に関する、また遠隔ローディングの順序を示す、すべての電話加入データにわたりサーチを行なう（ステージＥ４３）。

【００７８】次いで、コード／デコード手段ＣＤＦは秘密電話加入データを特別のキーの助けを得てコード化する（ステージＥ４４）。

【００７９】最後に、処理手段ＵＴＦは、秘密では無い公開電話加入データをコード化された秘密データと共に独立局ＳＰに遠隔ローディングの順序を示すデータの値の関数として送信することを許可する（ステージＥ６）。

【００８０】他方、呼び出し要求のための公開数値ワードＬＩＤが自動的に生成される場合は、それは独立局が電話加入データを要求しないか、あるいは既に個人として特定されていることを意味する。

【００８１】独立局からの認証の証明結果に応じて、認証センターの処理手段は電話接続の生成を許可するか、あるいは独立局からの呼び出し要求をさらに取り扱うことをしない（ステージＥ５）。

【００８２】より詳しく言えば、認証証明の要求は次のように展開する。

【００８３】認証要求のための数値ワードＡＵＴＨ＿ＲＥＳに応じて、認証センターのコード／デコード手段ＣＤＦは受けとられたランダムキーワード、すなわちコード化されたＣＰＩＮ、を特別キーＰＩＮの助けによりデコードし、このようにデコードしたランダムキーワードを生成されたランダムキーワードと比較し、比較の関数として、電話接続の生成を許可する。

【００８４】遠隔ローディングの順序を表すデータの値により独立局が遠隔的にロードされるべきであることが示される時、ステージＥ６がその役割を果たす。

【００８５】電話加入データの発信は２つの部分、すなわち１つは公開電話加入データに関する部分、そしてもう１つは秘密電話加入データに関する部分に分けることは非常に有利である。

【００８６】ステージＥ６１の時、数値ワードＴＲＤ＿ＡＬＬＯＣの発信により電話加入データＴＲＤの発信が可能である。

【００８７】秘密電話加入データの方は、数値ワードＰＩＮ＿ＡＬＬＯＣにより発信される。

【００８８】本発明によれば、秘密電話加入データはその秘密データが不正に横取りされることを避けるためコード化されて発信される。

【００８９】本発明によれば、秘密電話加入データのコーディングは、その独立局のための特別キーの選択が可

能な手段と共に、認証センターのデータコード／デコード手段により達成される。

【００９０】次に図４が参照される。

【００９１】ここで、秘密電話加入データのコーディングに用いられる特別キーはキーＥＰＩＤ（暗号化された携帯特定データ、Encrypted Portable Identification Data）である。

【００９２】勿論、この独立局のための特別キーＥＰＩＤは、独立局ＳＰと認証センターＣＡにおいて同時に格納されている。

【００９３】実際的には、認証センターの制御手段が、それぞれ３２ビットのサイズを有する第１および第２のランダム数ＥＰＩＮ１およびＥＰＩＮ２を最初に生成する。

【００９４】次いで、制御手段が、変換Ｓ１と、変換Ｓ２と2^{32}の積との和の助けを得て（秘密加入データを表す）個人特定番号ＰＩＮを生成し、それにより６４ビットからなるＰＩＮを得ることができる。

【００９５】場合によっては、制御手段は６４ビットの値の補足的変数データＥＰＩＮ３の助けを更に得てＰＩＮを生成するが、このＥＰＩＮ３は、やはり制御手段により生成され、排他的論理和によって前記の計算を完成するものである。

【００９６】このように、秘密電話加入データをコード化した仕方で遠隔ローディングするのを可能とするのは、変数ワードＥＰＩＮ１、ＥＰＩＮ２そして（場合により）ＥＰＩＮ３である。

【００９７】これらのワードＥＰＩＮ１、ＥＰＩＮ２そして（場合により）ＥＰＩＮ３を受け取ると、独立局のコード／デコード手段はまず第１に暗号関数Ｆを用い、秘密キーＥＰＩＤの助けを得てワードＥＰＩＮ１、ＥＰＩＮ２のそれぞれの変換Ｓ１とＳ２を計算する。最後に、Ｓ１、Ｓ２そして（場合により）ＥＰＩＮ３の助けにより秘密加入データＰＩＮを回復するための計算が行なわれる。

【００９８】秘密ならびに公開電話加入データが独立局において正しく遠隔的にロードされたことを証明するために、先に説明したステージＥ２３と同じ、認証要求のためのステージＥ８１が提供される。言い替えれば、このステージは、認証要求のための数値ワードＡＵＴＨ＿ＲＥＱをランダム数ＲＡＮＤと共に独立局へ送ることを含むものである。

【００９９】認証要求のための数値ワードＡＵＴＨ＿ＲＥＱに応じて、独立局のコード／デコード手段ＣＤＰは受け取ったばかりのランダムキーワードＲＡＮＤを、独立局に関する秘密加入データＰＩＮの助けによりコード化する。この秘密加入データＰＩＮは前にワードＥＰＩＮ１、ＥＰＩＮ２そしてＥＰＩＮ３を中間形態としてコード化されて発信されたものであり、キーＥＰＩＤを介してデコードされたものである。

【０１００】次いで、独立局ＳＰは、このようにコード化されたランダムキーワードＣＰＩＮを認証応答のための数値ワードＡＵＴＨ＿ＲＥＳと共に認証センターＣＡに送る。この認証応答のための数値ワードＡＵＴＨ＿ＲＥＳに応じて、認証センターのコード／デコード手段は、このようにして受け取ったコード化されたランダムキーワードＣＰＩＮを特別キーＰＩＮの助けを得てデコードする。最後に、認証センターはこのようにデコードされたランダムキーワードを生成されたランダムキーワードと比較し（ステージＥ８２）、比較結果に応じて電話接続を確立する（ステージＥ９）。

【０１０１】実際的には、１つの１バイトの公開数値ワードＵＳＥをデータの性質を示すためのものとすることが考えられる。例えば、バイトの第１ビットをデータのコーディングに関するものとする（０はコード化されておらず、１はコード化されていることを示す）。バイトの第２ビットは加入の性質に関するものとする（０はメイン、１は補助、言い替えれば、後に詳しく説明されるＲＯＡＭＩＮＧサービスを示す）。他のビットは独立局のそれぞれのメモリーにデータを格納するため０に維持される。

【０１０２】独立局に公開数値ワードＰＩＮ＿ＡＬＬＯＣの利用を示すのはワードＵＳＥであることに注目すべきである。

【０１０３】同様に、１つの１バイトの数値ワードＡＵＴＨ＿ＮＯの利用を考えることができる。この機能はデータをコード／デコードするために独立局にその暗号関数のうちどれを用いるべきかを示すことにある。もし独立局が利用できる１つの暗号関数だけしか持っていないのであれば、ワードＡＵＴＨ＿ＮＯの効果は無い。

【０１０４】先に説明した実施例においては、メッセージＰＩＮ＿ＡＬＬＯＣおよびＴＲＤ＿ＡＬＬＯＣを介して公開ならびに秘密電話加入データのローディングの開始を可能とするのは、キーボードから入力され、独立局から出される呼び出し要求のためのワードＬＩＤである。

【０１０５】この例においては、受話器がフックから外される時、自動的に独立局により生成されるワードＬＩＤは、その電話加入データの遠隔ローディングを可能としない。

【０１０６】その結果、独立局の利用者が望む場合（つまり、ここでは、キーボードからＬＩＤが入力された場合）にだけ、電話加入データが遠隔送信される。

【０１０７】独立局（あるいはその加入者）がどんな制御にも影響を与えることなく、あるいはどんな特定のサービスを要求することなく、電話加入データの少なくとも一部を修正する場合などの特定の適用の場合のために、遠隔ローディング方法を開始させるロード要求信号は認証手段からのロード要求とすることができる。

【０１０８】本発明の他の実施例によれば、電話加入デ

ータの遠隔ローディング方法は複数のポアンテル契約者の間のＲＯＡＭＩＮＧと称されるサービス（つまり、その独立局が加入していない補助的な電話ネットワークに対する呼び出し要求）にも適用される。

【０１０９】一般的に言って、ＲＯＡＭＩＮＧサービスは、ポアンテル契約者に対する特別の加入を申し込んだ独立局の加入者に他のポアンテル契約者の補助的な交換ネットワークをある程度利用することを認めるものである。ここで、ＲＯＡＭＩＮＧサービスは、その独立局に関するすべての公開および秘密データがその独立局のレベルと認証センターのレベルで同時に利用できる時にのみ可能であることに注意すべきである。

【０１１０】他方、不正接続を避けるため、補助的交換ネットワークを運営する補助的認証センターはその独立局の電話加入データを持たない。

【０１１１】これまでのところ、独立局の加入者が補助的ネットワークの運営者との接続を確立するとき、補助的認証センターは認証センターから、ランダムワードと秘密キーによるその変換からなる１対の認証規格を要求している。秘密キーは通常独立局の秘密電話加入データ、例えば個人特定番号ＰＩＮにより形成されている。

【０１１２】この１対の認証により独立局の補助センターレベルでの認証が可能である。

【０１１３】しかし、この認証方法による独立局の認証は次の理由で十分満足の行くものではない。

【０１１４】すなわち、一方では各認証センターのためのデータベースを形成するメモリーの間の交信はそれらが、各呼び出しの際、比較的長く、また体系的なものであるため、高い費用がかさむ。

【０１１５】他方、この認証方法は、独立局の認証を確認するためのデータベースを形成するメモリーを固定ターミナルが有する交換電話ネットワークには適切ではない。

【０１１６】出願人は、これらの不利な点を克服することのできる、ＲＯＡＭＩＮＧサービスにおける電話加入データの遠距離ローディング方法を提供するという問題に直面した。

【０１１７】本発明によれば、図１および図４を参照して説明された発明に調和してコード化された秘密電話加入データＰＩＮを送信するという原理は、補助認証センターが独立局と補助交換電話ネットワークとの間の電話接続を認証するために必要なメインの認証センターから補助認証センターへの仮秘密電話加入データの送信に適用される。

【０１１８】このように、仮秘密電話加入データは送信の前に独立局のための特別キーの助けによりコード化される。特別キーが独立局とメインの認証センターに同時に格納されている秘密電話加入データＰＩＮから形成されるのは有利である。

【０１１９】図５には、独立局と独立局がそのための電

話加入データを有しない補助交換電話ネットワークとが相互電話通話をしている電話装置が略図的に示されている（いわゆるＲＯＡＭＩＮＧサービス）。

【０１２０】独立局ＳＰは補助電話装置と遠隔通話が可能である。この補助電話装置の主要構成要素は図１を参照して説明された電話装置のものと同一であり、同じ参照符号に添字Ａを加えて示されている。

【０１２１】メイン認証センターＣＡは補助認証センターＣＡＡと数値信号接続ＬＣＡＡを介して接続されている。

【０１２２】ＲＯＡＭＩＮＧサービスにおいては、電話加入データの遠隔ローディングは、メイン認証センターＣＡが補助認証センターＣＡＡに数値信号接続ＬＣＡＡを介して接続されているときだけ可能である。

【０１２３】電話加入データの遠隔ローディングは補助認証センターがメイン認証センターと協調して稼働しているときにのみ可能であることに注意すべきである。

【０１２４】図６には、ＲＯＡＭＩＮＧサービスの枠組における仮秘密電話加入データの遠隔ローディングのプロトコルの主要な要素ステップが略図的に示されている。

【０１２５】ＲＯＡＭＩＮＧサービスの枠組における遠隔ローディングのプロトコルの開始は、ここではステージＥ１Ｒ、Ｅ２ＲおよびＥ３Ｒから成り立っており、図３に言及して説明されたプロトコルの開始（ステージＥ１、Ｅ２、Ｅ３）と同一である。異なっているのは、電話呼び出し番号のフォーマットを囲むＲＯＡＭＩＮＧキーボードの始動だけである。

【０１２６】独立局からの呼び出し要求（ステージＥ１Ｒ、Ｅ２ＲおよびＥ３Ｒ）の後、固定ターミナルは、補助認証センターにより運営される補助交換ネットワークと電話通信を確立するために認証要求を補助認証センターＣＡＡに提出する（ステージＥ４Ｒ）。

【０１２７】ステージＥ４に関する電話通信を確立する許可の要求は図３を参照して説明された認証の要求に等しい（ステージＥ４Ｒ）。ＲＯＡＭＩＮＧ情報の追加だけが異なっている。

【０１２８】補助認証センターが補助認証の問題であることを見いだせば、その補助認証センターは、独立局と補助交換電話ネットワークの間に電話接続を生成するためメイン認証センターからの許可を求めることを意図して認証要求を提出する。

【０１２９】補助認証センターからの認証要求（ステージＥ５Ｒ）に応じて、認証センターの制御手段は、まず第１に、それぞれ３２ビットの価を持つ第１および第２のランダム数ＥＰＩＮ１およびＥＰＩＮ２を生成する。

【０１３０】次に、認証センターのコード／デコード手段ＣＤＦは、暗号関数Ｆにより、（例えば本発明の方法による遠隔ローディングを通して駐在し、その機能を果たすため独立局のメモリーに格納された独立局の秘密電

話加入データを表す）秘密キーＰＩＮの助けを得て、その第１および第２のランダム数ＥＰＩＮ１およびＥＰＩＮ２のそれぞれの変換Ｓ１およびＳ２を計算する。

【０１３１】最後に、呼び出し要求のための公開数値ワードが独立局の認証に関する所定の条件を実証する時、認証センターの処理手段は変数データＥＰＩＮ１およびＥＰＩＮ２およびその変換Ｓ１およびＳ２の補助認証センターへの送信を許可する（ステージＥ６Ｒ）。

【０１３２】データＥＰＩＮ１およびＥＰＩＮ２、Ｓ１およびＳ２の送信に続いて、補助認証センターの制御手段ＭＣＦＡは、公開仮電話加入データを生成し、それらを補助固定ターミナルＢＦＡを介して独立局へと送信する。

【０１３３】さらに、制御手段ＭＣＦＡは、６４ビットのＰＲＩＮを得るため変換Ｓ１と、変換Ｓ２に2^{32}を掛けたものとの和の助けを得て、（秘密仮電話加入データを表す）個人特定番号ＲＰＩＮを生成する（ステージＥ７Ｒ）。

【０１３４】場合により、制御手段ＭＣＦＡは、やはり制御手段により生成され、上記の計算を排他的論理和により完成する、６４ビットの価を持つ補足的変数データＥＰＩＮの助けをさらに得て、ＰＲＩＮを生成する。

【０１３５】このように、一方では、補助認証手段のレベルにおける秘密仮データの生成が可能であるのは、変数ワードＥＰＩＮ１およびＥＰＩＮ２およびそれらの変換Ｓ１およびＳ２の送信による。他方、秘密仮電話加入データの遠隔ローディングが可能であるのは、補助手段と独立局間の変数ワードＥＰＩＮ１、ＥＰＩＮ２および（場合により）ＥＰＩＮ３の送信による。

【０１３６】ワードＥＰＩＮ１、ＥＰＩＮ２および（場合により）ＥＰＩＮ３の受け取りにより、独立局のコード／デコード手段は、第一に、秘密キーＰＩＮの助けを得て、暗号関数Ｆより、ワードＥＰＩＮ１およびＥＰＩＮ２のそれぞれの変換Ｓ１およびＳ２を計算する。最後にそれらは、秘密仮電話データＰＲＩＮの回復のための計算に終わる（ステージＥ９Ｒ、Ｅ１０Ｒ）。

【０１３７】最後に、このように受けとられた秘密でない仮公開電話加入データ、およびこのようにデコードされた秘密データはそれぞれのメモリーに格納される（ステージＥ１０Ｒ）。

【０１３８】ステージＥ６の後、補助認証センターは、独立局の認証を可能にする仮秘密電話加入データＲＰＩＮを有する。その結果、メイン認証センターによる補助認証センターの体系的な問い合わせはもはや必要ではない。

【０１３９】残りについては、補助認証センターによる独立局の認証に関するステージはメイン認証センターによる独立局の認証に関するステージと同一である。唯一の違いは、補助認証センターのレベルにおける仮公開電話加入データの生成にある。

【０１４０】補助認証手段が固定ターミナルに収納され、一般補助認証センターに接続されている場合は、本発明によれば、秘密仮電話加入データを補助認証手段のレベルで生成することを可能にするデータＥＰＩＮ１、ＥＰＩＮ２、Ｓ１およびＳ２を受け取る目的のため、その固定ターミナルが一般補助認証センターを問い合わせる手段が備えられているようにすることができる。

【図面の簡単な説明】

【図１】本発明の電話装置の略図である。

【図２】本発明による電話加入データの遠隔ローディングに関するプロトコルを示す線図である。

【図３】本発明による独立局と固定ターミナル間のデータの交換を示す線図である。

【図４】秘密電話加入データのコード／デコードを示す線図である。

【図５】独立局が補助的交換電話ネットワークと相互に作用する本発明の電話装置を示す線図である。

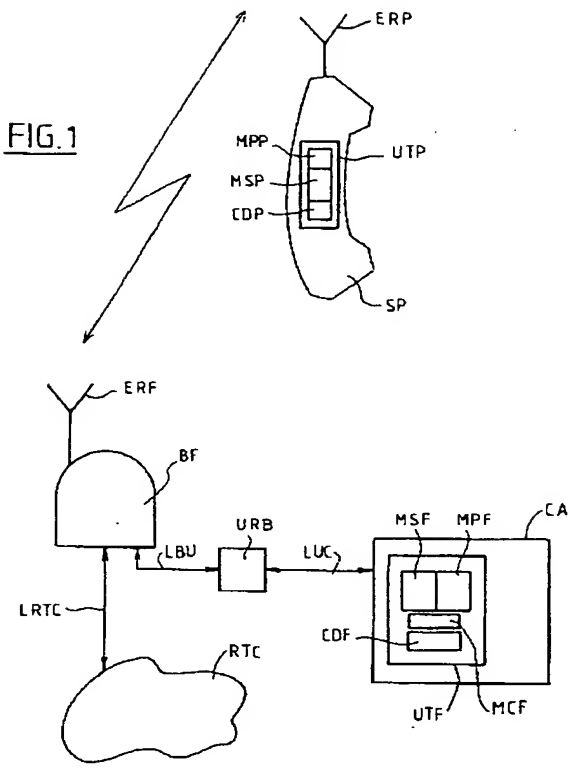
【図６】図５の装置における、電話加入データの遠隔ローディングに関するプロトコルを示す線図である。

【符号の説明】

ＢＦ　固定ターミナル
ＣＡ　認証手段
ＣＤＦ　コード／デコード手段
ＣＤＰ　コード／デコード手段
ＥＰＩＤ　特別キー
ＬＩＤ　呼び出し要求のための公開数値ワード
ＭＣＦ　制御手段
ＭＰＦ　メモリー
ＭＰＰ　メモリー
ＭＳＦ　メモリー
ＭＳＰ　メモリー
ＰＩＤ　独立局を特定するための公開数値ワード
ＰＩＮ　秘密特別キー
ＲＴＣ　交換電話ネットワーク
ＳＰ　独立局
ＵＴＦ　制御手段
ＵＴＰ　処理手段

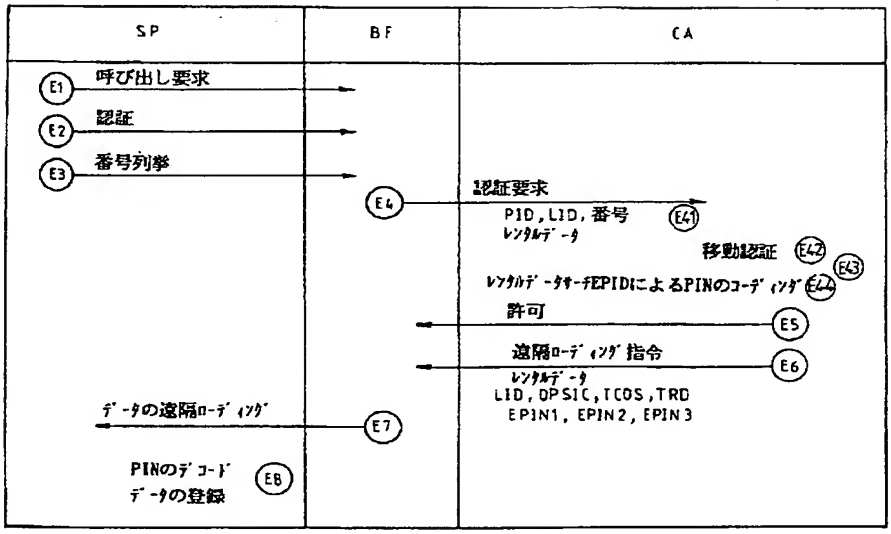
【図１】

FIG.1



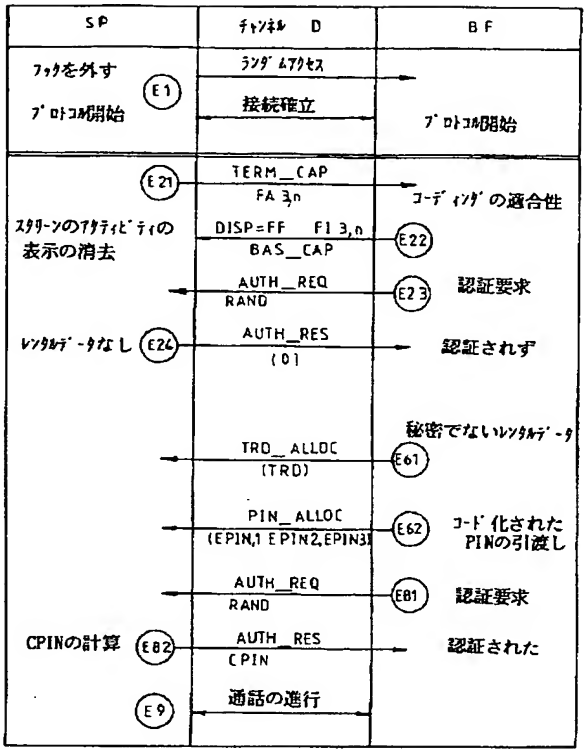
【図２】

FIG.2



【図３】

FIG.3



【図４】

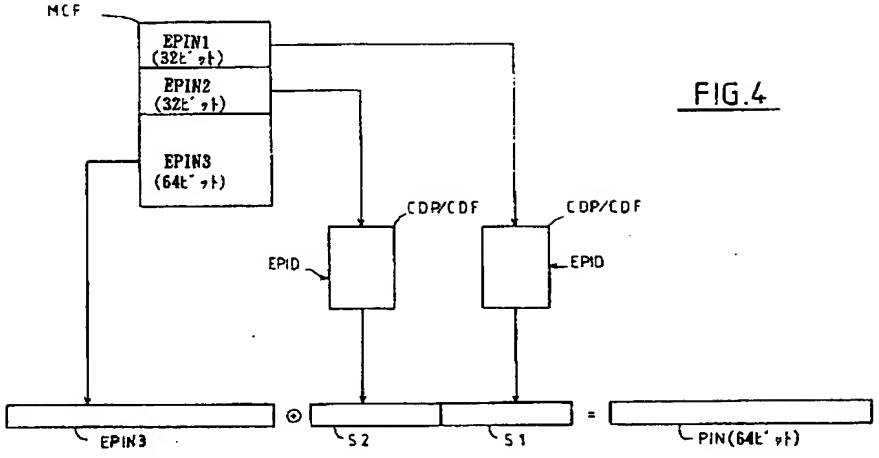


FIG.4

【図５】

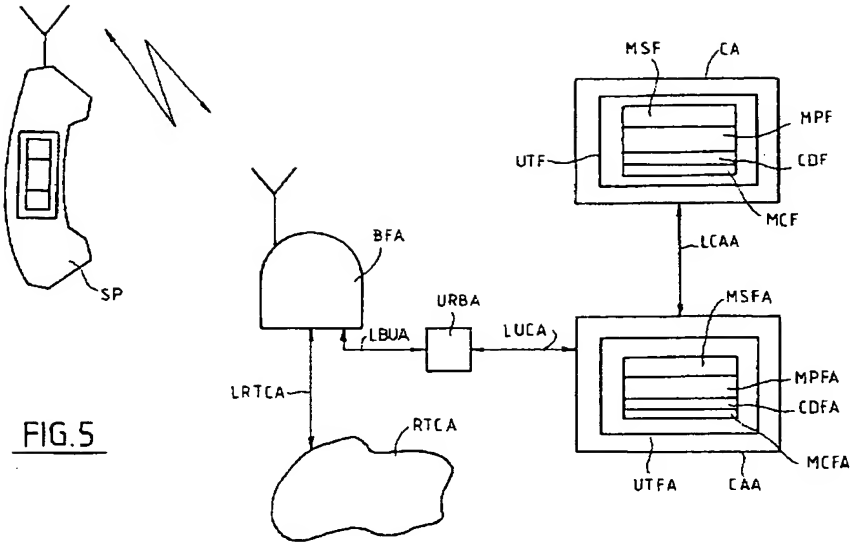


FIG.5

【図６】

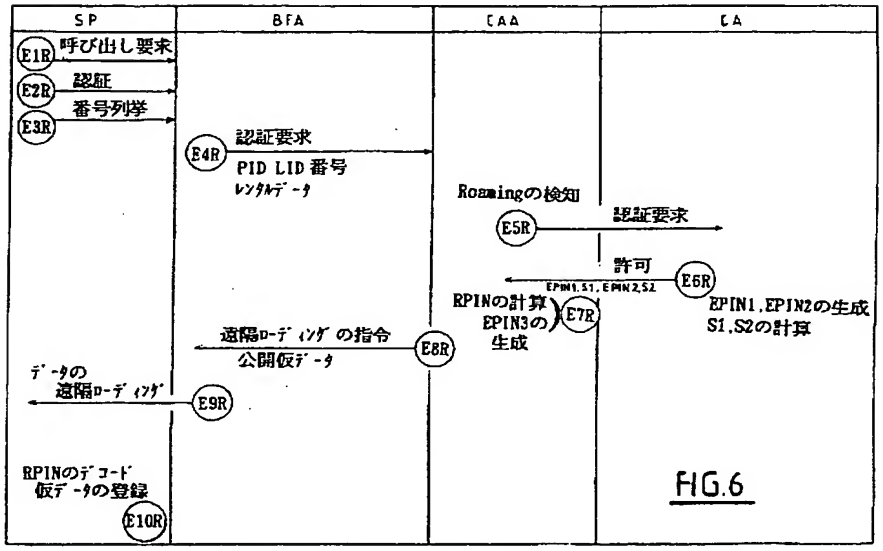


FIG.6

フロントページの続き

(72)発明者　ソフィー・ボードゥ
フランス国、エフー75013　パリ、リュ・
デ・コルデリエール、32